Computer Science

COMPARING PRIVACY PROPERTIES OF MIXNET AUDITS USED BY END-TO-END VOTING SYSTEMS, P. L. Vora*, B. Hosp, J. R. Rubio, George Washington University, Department of Computer Science, Washington, DC 20052, poorvi@gwu.edu

End-to-end voting systems allow voters to determine that their votes were correctly included in the tally, without revealing individual votes. A key component of a number of these systems is the mixnet, which shuffles encrypted votes and provides decrypted votes to a public website. These votes may then be counted by anyone. Our research has focused on the privacy properties of end-to-end voting systems that use mixnets.

In order to determine that a mixnet has correctly shuffled and decrypted votes, a number of end-to-end systems---such as Pret-a-Voter, PunchScan and Scantegrity---use a mixnet audit known as a randomized partial audit. Randomized partial audits performed on mixnets reveal information that is useful to an adversary who wishes to determine how the voter voted. Note that the audits will typically not reveal the individual vote, but will reveal information in order to improve the adversary's guess. Note further that these audits reveal information even when the cryptographic schemes used are secure, and the adversary is assumed to be computationally bounded.

Mixnets consist of a series of mixes. Each mix processes and shuffles encrypted votes, such that all votes are decrypted at the output of the last mix. If the shuffles are secret, an output decrypted vote cannot be linked to the corresponding input encrypted vote. In order to ensure that the mixnet did perform the processing correctly, a randomized partial audit is performed. The audit involves opening mixnet links. The manner in which the links are opened determines the type of audit. In an independent-link audit, each link is chosen with a certain pre-specified probability. In an alternating pair audit, half of the links in the first mix are chosen to be opened at random; the complementary links are chosen for the next mix and so on.

This research focuses on how successful an attacker is in guessing the chosen candidate of a voter for a given election depending on whether the election uses an independent-link audit or a complementary-half audit. Results were obtained by simulations that compared these audits given the same input variables. The improvement for complementary-half audits is dependent on the number of voters in the election; it is smaller for a larger number of voters. On the other hand, the improvement for independent-link audits depends on the number of mixes and decreases for a larger number of mixes. Therefore, elections with a limited number of mixes should use complementary-half audits, while elections with few voters and a large number of mixes should use independent-link audits. These results, obtained using simulations, are consistent with the theoretical results observed by Hosp and Vora.

J. R. Rubio was supported by NSF-REU grant No. CNS-0831149